КРИМИНАЛИСТИКА

УДК 343.985.7

Криминалистические особенности способов совершения хищений с применением методов социальной инженерии и информационно-телекоммуникационных технологий

Н. И. Старостенко

Краснодарский университет МВД России,
Российская Федерация, 350005, Краснодар, ул. Ярославская, 128

Для цитирования: Старостенко, Нина И. 2024. «Криминалистические особенности способов совершения хищений с применением методов социальной инженерии и информационно-телекоммуникационных технологий». *Вестник Санкт-Петербургского университета. Право* 1: 152–170. https://doi.org/10.21638/spbu14.2024.110

В статье представлена криминалистическая характеристика системы действий преступника по подготовке, совершению и сокрытию хищений, совершаемых с применением методов социальной инженерии и информационно-телекоммуникационных технологий. Автор анализирует судебную и следственную практику и выявляет основные виды хищений с использованием методов социальной инженерии и информационно-телекоммуникационных технологий. Описываются основные методы социальной инженерии, которые наиболее часто используют преступники для установления психологического контакта и оказания воздействия на психику и поведение жертв. Анализ способов совершения указанных хищений позволил выявить их закономерные связи с другими элементами криминалистической характеристики, в частности с личностью преступника, личностью потерпевшего, механизмом следообразования и др. В статье представлена криминалистическая характеристика личности преступника и его противоправной деятельности. На основе специальной литературы и судебно-следственной практики сформулирована криминалистическая классификация способов совершения хищений с применением методов социальной инженерии и информационно-телекоммуникационных технологий. Раскрыто содержание методов социальной инженерии, включающих в себя психологические и технологические приемы манипуляции. Непосредственное совершение противоправных действий наряду с применением методов социальной инженерии характеризуется использованием средств сотовой и иных видов голосовой связи, программ удаленного администрирования, интернет-

сайтов, сервисов электронной почты и мгновенного обмена сообщениями, приложений социальных сетей и др. Подводя итоги, автор делает вывод о том, что в общем виде рассматриваемые способы являются полноструктурными, поскольку в их содержание включен определенный набор действий (этапов): подготовка, непосредственное совершение противоправных действий, сокрытие следов преступления.

Ключевые слова: криминалистика, расследование преступлений, социальная инженерия, методы социальной инженерии, дистанционное мошенничество, способы совершения хищений, информационно-телекоммуникационные технологии.

1. Введение

Информационно-телекоммуникационные технологии приобрели глобальный трансграничный характер и стали неотъемлемой частью всех сфер деятельности личности, общества и государства. Их эффективное применение является фактором ускорения экономического развития государства и формирования информационного общества[1]. Вместе с тем современное состояние преступности в мире характеризуется устойчивым ростом преступных проявлений, связанных с использованием в противоправной деятельности информационно-телекоммуникационных технологий. При этом виртуальный мир меняет уклад механизмов совершения преступлений различного вида, способствует переходу от традиционных, простых способов их совершения к более сложным формам. Так, несмотря на то что появляются новые методы защиты от дистанционных действий злоумышленников, а также активно вскрываются преступные схемы в информационном пространстве, на противодействие рассматриваемой преступности оказывают влияние постоянное развитие информационных технологий, использование психологических манипуляций и современных программных продуктов. Действительно, внедрение в противоправную деятельность различных программных средств, в том числе технологий искусственного интеллекта, может существенно менять характер преступности, открывать новые криминальные возможности, облегчать достижение целей, совершенствовать способы подготовки и совершения преступлений[2].

Основную часть среди преступлений рассматриваемого вида составляют хищения, причем в процессе совершения данных преступлений злоумышленники все чаще применяют различные психологические приемы и уловки, которые называются методами социальной инженерии.

В специальной литературе существуют различные определения социальной инженерии, обобщив которые можно констатировать, что она представляет собой приемы обмана и психологического манипулирования людьми в целях осуществления контроля за их поведением или действиями (Резник 1994; Ревенков, Бердюгин 2017; Овчинский 2016, 47).

Основная особенность преступлений подобного рода состоит в том, что они совершаются лицами, обладающими знаниями в области психологии, а также уме-

[1] Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». Здесь и далее все ссылки на российские нормативно-правовые акты и судебную практику приводятся по СПС «Гарант». Дата обращения Дата обращения 1 февраля, 2024. http://base.garant.ru.

[2] В настоящей статье использовались ранее не опубликованные фрагменты диссертационного исследования (Старостенко 2023).

ниями собирать необходимую информацию о жертвах для реализации корыстных целей. Вместе с тем способ совершения преступлений данной категории обусловлен разработкой злоумышленниками специальных алгоритмов и сценариев обмана, направленных на их многократное применение в отношении граждан. К тому же совершению данных преступлений предшествует длительная и тщательная подготовка, в процессе которой преступник заранее продумывает способы сокрытия следов преступных действий, препятствующих своевременному установлению лиц и фактов, представляющих интерес для криминалистов.

Способы совершения хищений с применением методов социальной инженерии рассматривались многими зарубежными авторами (Blommaert, Omoniyi 2006; Huang, Brockman 2011; King, Thomas 2009; Mann 2008; Ross 2009; Workman 2009; Zook 2007; и др.), однако в отечественных научных трудах указанное преступное явление детально не изучено, в частности отсутствует классификация способов его совершения.

В настоящем исследовании криминалистическая классификация способов совершения хищений с применением методов социальной инженерии и информационно-телекоммуникационных технологий проводится на основании анализа вступивших в силу 72 приговоров судов и 60 уголовных дел, возбужденных на территории Краснодарского края и Республики Адыгея, а также материалов из более 500 уголовных дел, касающихся фактов совершениях хищений электронных денежных средств с использованием методов социальной инженерии. Кроме того, нами проведены опросы сотрудников следственных подразделений, проходящих службу на территории 12 субъектов РФ, о содержании основных способов совершения хищений анализируемого вида, с которыми они сталкивались наиболее часто.

2. Основное исследование

2.1. Личность преступника, совершающего хищения электронных денежных средств с использованием методов социальной инженерии

Личность злоумышленника, а также криминалистическая характеристика его преступной деятельности играют основную роль в механизме совершения преступлений любой категории.

В криминалистике общепринято представление о личности преступника как о системе биологических (антропологических, анатомических, биохимических, функциональных), социальных (общегражданских, семейно-бытовых, профессиональных, антиобщественных) и психических (психологических, психопатологических) свойств человека, сведения о которых отражены в окружающей среде и могут оказать существенное влияние на организацию поисково-познавательной деятельности по раскрытию и расследованию преступлений (Комиссарова 2016, 224).

Определив специфику преступности указанного вида, мы пришли к выводу, что необходимо проанализировать ряд профессиональных навыков и социально-психологических характеристик личности злоумышленников, так как именно эти особенности влияют на умения владения компьютерной техникой, программными

средствами и технологиями, способствуют оказанию психологического воздействия на жертв в момент совершения преступления.

Личность преступника, совершающего хищения с использованием методов социальной инженерии, характеризуется в первую очередь более длительной подготовленностью к совершению преступлений, обусловленной приобретением знаний в области психологии общения, психиатрии, физиологии, криминальных навыков обмана либо психологического манипулирования людьми и умений использовать указанные знания при реализации корыстного умысла. Вместе с тем субъект рассматриваемой криминальной деятельности характеризуется широкими коммуникативными способностями, навыками установления психологического контакта с потенциальной жертвой. При установлении психологического контакта с жертвой злоумышленники ведут себя уверенно, имеют подставленный голос, используют терминологию из различных сфер деятельности — банковской, правоохранительной или иной, соответствующей преступной легенде.

Выбор схемы преступного поведения (например, поведение кредитного специалиста банка) обусловлен углубленным представлением о деятельности того или иного специалиста. Так, перед совершением хищений с применением методов социальной инженерии преступник может осуществлять поиск необходимой для обмана информации в сети Интернет и социальных сетях. Указанные сведения, как правило, изучаются на этапе подготовки к совершению преступления. Такая информация может включать в себя персональные данные потенциальных жертв, данные аккаунта из социальных сетей, правила делового общения, сведения о банковской деятельности, знания прав и обязанностей сотрудника банка, организационной структуры и полномочий органов государственной власти. Получение подобных сведений и умелое их использование в процессе обмана позволяют преступникам маскировать корыстные намерения под правомерные действия. Следовательно, чем больше информации о личности потенциальной жертвы, ее интересах, а также об исполняемой роли злоумышленник может получить, тем выше вероятность совершения хищения денежных средств.

В большинстве случаев воздействие на потерпевшего с применением методов социальной инженерии осуществляется дистанционно, путем использования средств сотовой связи, электронной почты, SMS-сообщений, мессенджеров или социальных сетей. Кроме того, злоумышленник обладает навыками обращения с компьютерной техникой, с различными программно-аппаратными средствами и вредоносным программным обеспечением, чтобы создать такие условия, при которых могут успешно реализовываться методы социальной инженерии. Также злоумышленник имеет широкие представления о принципах функционирования сервисов дистанционного банковского обслуживания и особенностях систем банковских уведомлений, он может обладать умениями в создании копий интернет-сайтов, в осуществлении подделок фото-, видеоизображений и голоса конкретного человека, применяя при этом специальные программные средства.

Преступления рассматриваемой группы зачастую характеризуются тем, что совершаются в соучастии. В таком случае преступная деятельность предполагает распределение между участниками группы функций и ролей по совершению совместных хищений денежных средств у граждан. В судебной и следственной практике отмечается, что такие группы могут объединяться для достижения общих

корыстных целей в специализированных помещениях, так называемых колцентрах. Там распределяются преступные роли, организуются рабочие места, подготавливаются тексты, необходимые для вступления во взаимодействие с жертвами, отрабатываются приемы психологического воздействия и т. д.

На повышение организованности преступности влияют особенности кибернетического пространства, поскольку они могут создавать условия для анонимности преступных действий, а уникальные возможности современных технологий позволяют координировать и объединять усилия для быстрого достижения общих корыстных целей, совместно использовать сеть Интернет для поиска потенциальных жертв и их конфиденциальных данных и т. п.

Таким образом, основные особенности личности преступника, совершающего хищения изучаемого вида, связанны с его психологическими, интеллектуальными характеристиками, а также с умениями и навыками использования технических возможностей электронных устройств и программных средств в преступной деятельности.

2.2. Подготовка к совершению хищений с использованием методов социальной инженерии и информационно-телекоммуникационных технологий

В криминалистической литературе достаточно подробно освещены вопросы, касающиеся способа совершения преступлений в общем виде. Большинство ученых отмечают, что необходимо рассматривать способ совершения преступлений как систему действий по подготовке, совершению и сокрытию преступления, которые детерминируются условиями внешней среды, а также психологическими и физиологическими свойствами личности, связанными с использованием определенных орудий, средств, условий места и времени (Аверьянова и др. 2000, 268).

Способы совершения хищений анализируемой категории также надлежит рассматривать в комплексе действий злоумышленника по подготовке к совершению преступления, непосредственному совершению, а также сокрытию.

Анализ судебной и следственной практики позволил установить, что при подготовке к совершению хищений с применением методов социальной инженерии и информационно-телекоммуникационных технологий злоумышленники осуществляют целый ряд действий.

При совершении хищений в форме соучастия подготовка к совершению преступления, как правило, заключается в поиске помещения, пригодного для организации рабочих мест, и их оснащении необходимой компьютерной техникой, средствами голосовой связи. Далее организатор преступной группы совершает поиск и отбор участников, обладающих соответствующими психологическими качествами личности, проводит их обучение, осуществляет распределение ролей, обязанностей, предоставляет тексты и сценарии обмана, необходимые для оказания психологического воздействия на жертв.

При подготовке к совершению хищений преступники уделяют отдельное внимание изучению литературы о психологии человека, методам оказания психологического воздействия на жертв, тактике определения психотипов собеседников по

структуре речи; кроме того, они отрабатывают навыки психологического воздействия на жертв посредством речевого или текстового манипулирования.

В процессе подготовки к совершению преступлений злоумышленники осуществляют поиск необходимой информации для обмана потенциальных жертв. К таким данным относятся сведения, позволяющие, например, обращаться к жертве по имени и отчеству для установления психологического контакта. Кроме того, преступники могут заранее из мессенджеров или страниц социальных сетей получать информацию о жертве (номер телефона, адрес электронной почты, личные фотографии, фотографии членов семьи, друзей, места работы, места жительства, сведения о текущем местоположении, об увлечениях и хобби и т. д.). Знание подобных данных, несомненно, способствует усилению психологического воздействия на жертву.

Вместе с тем на этапе подготовке к совершению данных преступлений преступники могут осуществлять разработку алгоритмов общения, необходимых для оказания психологического воздействия на жертв, сценариев обмана, готовить специальные тексты. Указанные материалы служат руководством для «начинающих» преступников. Причем данные тексты и алгоритмы злоумышленники зачастую заучивают наизусть, отрабатывают их чтение с соблюдением необходимой интонации.

> Так, из Приговора Железнодорожного районного суда города Барнаула, Алтайского края от 28.07.2020 по делу № 1-93/2020 следует, что П. В. и Б. покушались на хищение чужого имущества путем обмана с причинением значительного ущерба гражданину организованной группой, выдавая себя за сотрудников банка. В целях реализации задуманного неустановленное лицо (организатор) разработало план совершения хищения, в соответствии с которым организованная группа под его руководством должна была: арендовать офисное помещение и оборудовать его компьютерной техникой, оснащенной доступом к сети Интернет; для осуществления звонков приискать мобильные телефоны и сим-карты, а также для зачисления и последующего обналичивания похищенных денежных средств приискать банковские карты, зарегистрированные в целях конспирации на третьих лиц; приискать информацию о гражданах, оставлявших в сети Интернет заявки на получение кредитов в банковских учреждениях, осуществляющих свою деятельность на территории РФ.

На данной стадии преступники, совершающие хищения с применением методов социальной инженерии и информационно-телекоммуникационных технологий, могут осуществлять приискание программных средств, необходимых для реализации корыстного умысла и сокрытия следов преступления. К таким программным средствам относятся программы, позволяющие выполнять подмену абонентского номера при осуществлении телефонных звонков, например Call Voice Changer — IntCall[3]; программы, позволяющие отправить SMS-сообщение с подменой абонентского номера отправителя (SMSBomba[4], SmsToo1[5], TipTopSMSWin[6]

[3] Call Voice Changer — IntCall. Дата обращения 1 февраля, 2024. https://apps.apple.com/ru/app/call-voice-changer-intcall/id535048805.

[4] SMSBomba 2.0. Дата обращения 1 февраля, 2024. https://soft.softodrom.ru/ap/SMSBomba-p12982.

[5] SMS Server Tools 3 — Project homepage. Дата обращения 1 февраля, 2024. http://smstools3.kekekasvi.com.

[6] TipTopMobile. Дата обращения 1 февраля, 2024. https://4pda.to/forum/index.php?showtopic=104549.

и др.); программы для удаленного доступа (AnyDesk[7] или TeamViewer[8]); VPN-сервисы; программные средства deepfake для создания аудио-, фото- и видеоматериалов с заменой лиц. Такие программы, как правило, находятся в открытом бесплатном доступе в сети Интернет; злоумышленник с легкостью может их установить на компьютерное или мобильное устройство и использовать при совершении преступлений. Эти программы заведомо направлены на сокрытие следов хищений и затрудняют идентификацию злоумышленника по голосу, абонентскому номеру, IP-адресу, а также по характеру выполняемых действий при использовании программ удаленного доступа.

Таким образом, совершение хищений с применением методов социальной инженерии и информационно-телекоммуникационных технологий предусматривает более тщательную подготовку, включающую в себя разработку сценариев и алгоритмов обмана потенциальных жертв, анализ психологических особенностей личности, изучение специальной литературы по психологии, поиск необходимых компьютерных или мобильных устройств, а также определенных программ, создающих необходимые условия для оказания психологического воздействия.

2.3. Совершение хищений с использованием методов социальной инженерии и информационно-телекоммуникационных технологий

Некоторые авторы выделяют популярные способы обмана посредством использования методов социальной инженерии: родственник в беде, обман в социальных сетях, покупка товаров или оплата услуг, обман на сайтах бесплатных объявлений, помощь в получении кредита (Кравченко 2019). Рассмотрим выявленные в ходе анализа эмпирического материала (по результатам анкетирования следователей дознавателей) основные способы непосредственного совершения хищений с применением методов социальной инженерии и информационно-телекоммуникационных технологий.

2.3.1. Убеждение жертвы в необходимости сообщить конфиденциальную информацию или совершить операцию по банковскому счету во время телефонного разговора

2.3.1.1. Убеждение потерпевшего предоставить банковские данные

Достижение корыстной цели в рассматриваемом способе совершения хищения происходит за счет добровольной передачи жертвой необходимых персональных данных или информации о банковской карте / банковском счете (CVV-код, срок действия банковской карты, пароль от личного кабинета сервиса дистанционного банковского обслуживания и др.), получая которые преступники самостоятельно могут осуществлять вход в личный кабинет сервиса дистанционного банковского обслуживания от имени жертвы, переводить денежные средства на свои счета, ис-

[7] AnyDesk. Дата обращения 1 февраля, 2024. https://anydesk.com/ru.
[8] TeamViewer. Дата обращения 1 февраля, 2024. https://www.teamviewer.com.

пользовать реквизиты банковской карты для осуществления различных финансовых операций, сделок и т. д. Кроме того, иногда преступникам для осуществления хищения денежных средств достаточно узнать код от банка, пришедший в SMS-сообщении.

Исполняя выбранную роль (например, сотрудник банка), они используют специально разработанные тексты (сценарии), которые необходимо проговаривать в момент телефонного разговора. Это позволяет создать специальные условия для реализации обмана, вывести человека из спокойного состояния и отключить у него логическое мышление. Также при совершении таких хищений преступники могут применять технологии подмены абонентских номеров телефона, позволяющих звонить жертвам с похожего номера или номера, идентичного номеру банковской организации (например, номер Сбербанка — 900).

2.3.1.2. Убеждение потерпевшего осуществить перевод денежных средств на определенный счет

Рассматриваемый способ хищения заключается в убеждении жертвы от имени службы безопасности банка либо кредитного специалиста выполнить срочный перевод в онлайн-кабинете банка или положить с помощью банкомата денежные средства на специальный страховочный (безопасный) счет в связи с возникшей утечкой конфиденциальных данных клиентов банка и большими рисками потери денежных средств, находящихся на банковском счете. Также практике известны случаи, когда злоумышленники представляются сотрудниками Центрального банка, МВД, ФСБ и сообщают о попытке оформления кредита на имя жертвы и о том, что для выхода из такой ситуации требуется немедленно выполнить определенные действия под контролем специалиста. В данной преступной схеме они указывают на сотрудника органа, который может вызвать доверие у конкретного человека в зависимости от сложившейся ситуации или предварительно собранной информации (сотрудник службы безопасности, прокуратуры). Зачастую с потерпевшим вступают во взаимодействие несколько злоумышленников, например один специалист безопасности банка, второй — кредитный специалист, которые согласованно вводят потерпевшего в заблуждение, сообщая ложную информацию.

Зачастую для создания доверительных отношений звонившие при обращении к жертве называли ее фамилию, имя и отчество, семейное положение, место жительства, последние четыре цифры кредитной карты и другую информацию, которую преступники предварительно собрали. В таком случае они надеются на совершение жертвой активных и необдуманных действий по банковскому счету для предотвращения мошеннической операции.

2.3.1.3. Убеждение потерпевшего оказать финансовою помощь «родственнику» или «другу»

При реализации корыстного умысла преступники предварительно разрабатывают алгоритм общения с жертвой, чтобы ввести ее в стрессовое состояние, и при звонках выдают себя за близкого родственника (внука/внучку, сына/дочь и др.) или друга, который, например, находится в больнице по причине того, что является

виновником дорожно-транспортного происшествия либо нуждается в срочной материальной помощи. Основная цель действий при осуществлении хищения денежных средств — убеждение жертвы в том, что человек, отправивший сообщение или говорящий по телефону, действительно является ее другом или близким родственником, которому требуется неотложная помощь в виде перевода денежных средств или оплаты лечения.

Для результативности применения специально разработанного алгоритма преступники могут изображать плач, называть жертву «мамой», создавать помехи сотовой связи и т. д. Также активно применяются программные средства, позволяющие скрытно и дистанционно оказывать психологическое воздействие на человека, в частности программы для изменения голоса, позволяющие моделировать голос плачущего ребенка, программы по изменению номера телефона, позволяющие изменить абонентский номер телефона и представить его как номер близкого родственника жертвы.

Вместе с тем при совершении хищений названным способом злоумышленники могут использовать для обмана полученные из социальных сетей данные о текущем местоположении лица или его планах покинуть город, страну. Получив такие сведения, преступник выдает себя за этого человека, звонит его родственникам или друзьям, рассказывая о том, что находится в тяжелой ситуации, в которую он попал в путешествии.

2.3.2. Внушение жертве необходимости установить программу, предоставляющую удаленный доступ к информации и управлению устройством

В рассматриваемом способе преступник обманом получает доступ к сервису дистанционного банковского обслуживания либо приобретает возможность просматривать SMS-сообщения, приходящие от банковской или кредитной организации.

Злоумышленник (под видом специалиста информационной безопасности, виртуального помощника, обеспечивающего защиту банковских вкладов, и пр.) предлагает установить программное (антивирусное) обеспечение, которое, по его словам, поможет оптимизировать работу с банковскими счетами или организовать защиту от мошеннических операций, вредоносных компьютерных программ и т. п. При этом преступник может называть эту программу «Поддержка Сбербанк», «Защитное приложение банка» и др. Однако на самом деле после установки жертвой программы он получает удаленный доступ ко всем данным, хранящимся в смартфоне, в том числе к сервису дистанционного банковского обслуживания, личным сообщениям от банка, приобретает возможность распоряжаться денежными средствами с банковских счетов и совершать сделки от имени потерпевшего.

Зачастую преступники используют легальную программу для делегирования доступа типа TeamViewer, которая позволяет стороннему лицу подключиться к компьютерному устройству или сотовому телефону (смартфону) жертвы. Главная опасность указанной схемы, предполагающей использование программ удаленного администрирования типа TeamViewer, заключается в том, что преступники, осуществляя удаленное управление смартфоном пользователя, могут за короткий

срок совершить хищение денежных средств — им достаточно убедить клиента банка установить и настроить программу для удаленного доступа под видом полезной утилиты, после чего все операции можно осуществлять удаленно с устройства пользователя (Крылов 2019).

Кроме того, таким же способом преступники могут скрытно установить на устройство пользователя вредоносное программное обеспечение, например троянскую программу, позволяющую им получать исчерпывающие данные об устройстве и его программном обеспечении, а самое главное — предоставляющие возможность перехватывать и отправлять SMS-сообщения от имени пользователя без его ведома (Кравец, Шувалов 2020).

> Так, неустановленное лицо, находясь в неустановленном месте, путем обмана под предлогом установки антивируса убедило П. установить на свой мобильный телефон программу, с помощью которой получило возможность просматривать SMS-сообщения от банка, тем самым получило доступ к личному кабинету «Росбанка» и завладело со счета денежными средствами П. в общей сумме 196 тыс. руб.[9]

2.3.3. Убеждение жертвы перейти по ссылке на определенный интернет-сайт

Особенностью данного способа является то, что злоумышленники создают сайты — копии порталов государственных услуг (например, «Госуслуги»[10]), известных магазинов, предлагающих товары по низкой стоимости, интернет-форм на оплату товаров, интернет-сервисов для размещения объявлений (например, «Авито. Доставка»[11], «Юла. Доставка»[12]) и под видом продавца/покупателя, представителя какой-либо организации убеждают потерпевших перейти по отправленной ссылке и ввести данные банковской карты, обусловливая это необходимостью получить какую-либо выплату, осуществить оплату товара, его доставку. Злоумышленники стремятся получить ФИО лица, которому принадлежит карта (счет), номер банковской карты (счета), CVV-код, срок действия банковской карты и др.

Сервисы объявлений создают условия, направленные на затруднение «работы» мошенников, вводя технические ограничения, например осуществляют защиту номера телефона или блокируют возможность вставлять в сообщения ссылки на внешние ресурсы, побуждают пользователей вести всю коммуникацию по сделкам внутри сервиса, не переходить в сторонние мессенджеры. Однако пользователи зачастую пренебрегают данными рекомендациями и в переписке в сервисе «Авито» добровольно сообщают преступникам свои номера телефонов, связываются с ними с помощью различных сервисов мгновенного обмена сообщениями, переходят по ссылкам на фишинговые ресурсы. Там «покупатель» подробно интересуется товаром и задает вопросы о его состоянии (когда приобрели, какие есть недостатки и др.), создавая впечатление, что реально заинтересован в покупке. Далее «покупа-

[9] Материалы уголовного дела № 1200103000400147, возбужденного 10.08.2020 СО ОВД ОМВД РФ по г. Анапе Краснодарского края по признакам, предусмотренным ч. 2 ст. 159 Уголовного кодекса РФ.

[10] Госуслуги. Дата обращения 1 февраля, 2024. https://www.gosuslugi.ru.

[11] Авито. Доставка. Дата обращения 1 февраля, 2024. https://www.avito.ru/dostavka.

[12] Юла. Доставка. Дата обращения 1 февраля, 2024. https://youla.ru/promo/delivery-terms.

тель» пишет, что он из другого города, и уточняет возможность отправки товара с помощью сервисов «Авито. Доставка», «Юла. Доставка». Продавец, как правило, соглашается, и «покупатель» проговаривает детали дальнейших действий, разработанных по определенному сценарию. Для большего доверия «покупатель» указывает в переписке, что он оформляет, оплачивает товар и направляет ссылку для получения денежных средств за продажу товара, далее жертва, переходя по «фишинговой» ссылке, передает реквизиты банковской карты, в том числе CVV-код, якобы для получения оплаты за товар (Рачева, Балеевских, Котов 2021).

Преступник может исполнять и роль «продавца» при размещении объявлений на подобных ресурсах. Для убедительности он может осуществлять приискание фотографий для размещения объявлений в своем профиле с несуществующими товарами/услугами, подготавливать тексты объявлений, содержащих выгодное предложение, ссылки на оплату товара и т. д.

Другой пример — схема, когда жертве направляется ссылка с заманчивым предложением о выгодной покупке в интернет-магазине, предлагающем товары с большой скидкой. Зачастую преступники создают копию известного магазина одежды или обуви, цифровой или бытовой техники. Особенностью такого сайта является то, что при оформлении покупки невозможно приобрести товар с оплатой после доставки, т. е. создаются условия, при которых жертва должна ввести данные банковской карты для оформления заказа.

Еще одна схема — рассылка по электронной почте сообщений, содержащих ссылку на фишинговый сайт (например, на копию сайтов «Госуслуги», «Налоги ФЛ»[13]). Преступники создают фишинговый сайт, полностью дублирующий интерфейс легитимного сайта, добавляют платежные формы для ввода жертвами данных своих банковских карт, логинов и паролей от сервисов дистанционного банковского обслуживания или от личного кабинета на портале государственных структур, формируют фишинговую ссылку для отправки. Отдельное место в данной схеме занимает текст рассылки. Преступник, исполняя, например, роль сотрудника социальной службы, отправляет жертве специально подготовленный текст от имени этой организации, содержащий данные о получении тех или иных выплат, пособий, социальной помощи, компенсаций и т. д., сообщает алгоритм действий, которые необходимо выполнить в определенной последовательности, включая переход по ссылке и предоставление своих конфиденциальных данных.

2.3.4. Доведение до жертвы недостоверной информации в социальных сетях

Основными направлениями совершения хищений с применением методов социальной инженерии в социальных сетях являются проведение розыгрыша подарков и денежных вознаграждений от имени блогера, сборы денежных средств на лечение тяжелобольного человека, обман в сфере онлайн-знакомств.

При совершении хищений указанным способом преступники создают копию страницы в социальных сетях от имени известных артистов, блогеров, проводящих конкурсы по розыгрышу подарков и денежных призов. Злоумышленники осущест-

[13] Личный кабинет налогоплательщика. Дата обращения 1 февраля, 2024. https://lkfl2.nalog.ru.

вляют приискание их фотографий для размещения, подготавливают тексты к таким фотографиям, «накручивают» подписчиков, друзей и лайки, т. е. большинство таких интернет-страниц создается искусственно с помощью специального программного обеспечения (Лихтер 2020). Данные действия выполняются преступниками для того, чтобы создать специальные условия, свидетельствующие о реальности выигрыша денежных средств или подарка, тем самым вызывая у жертв желание сообщить сведения банковской карты или оплатить доставку выигранного приза.

Кроме того, преступники создают профили (персональные страницы в социальных сетях), содержащие ложную информацию о срочных сборах на лечение. При этом для правдоподобности и соблюдения модели поведения человека, нуждающегося в финансовой помощи на лечение, злоумышленники используют фотографии людей, находящихся в трудной жизненной ситуации, медицинские документы, свидетельствующие о диагнозе.

> Так, К. под псевдонимом aidahubieva разместила в социальной сети Instagram* объявление, содержащее заведомо ложные сведения о том, что тяжелобольному ребенку необходимо собрать денежные средства, приложив к объявлению имевшуюся в свободном доступе в сети Интернет фотографию детей с ложными сведениями о наличии вымышленного заболевания «острый миелодный лейкоз М7» и указав реквизиты банковской карты своего брата С., к лицевому счету которого она имела доступ. Тем самым К. ввела в заблуждение относительно истинных намерений, а также своей личности Х., ввиду чего 14.08.2018 и 30.12.2018 на указанную в объявлении К. банковскую карту Сбербанка России (номер обезличен) были переведены денежные средства в общей сумме 8 тыс. руб. посредством приложения «Мобильный банк», установленного на мобильном телефоне Х., с банковской карты Сбербанка России (номер обезличен), оформленной на имя сестры Х. Обратив указанную сумму в свою пользу, К. распорядилась ею по своему усмотрению, чем причинила Х. значительный материальный ущерб[14].

Другой схемой совершения хищений денежных средств с применением методов социальной инженерии в социальных сетях является обман при онлайн-знакомствах. Преступные действия злоумышленника в данном случае предусматривают действие по заранее спланированному сценарию, включающему поиск и подготовку фотографий третьих лиц, создание аккаунта с размещением указанных фотографий на сайте знакомств (или страницы в социальной сети) от имени вымышленного человека, формирование текстовых клише для вступления во взаимодействие с потенциальными жертвами с целью заведения знакомств и последующего осуществления просьб в оказании финансовой помощи и т. д.

Таким образом, методы социальной инженерии, применяемые при совершении хищений с использованием информационно-телекоммуникационных технологий, — это совокупность психологических приемов, технических действий по применению программных средств, технологий в процессе подготовки, непосредственного совершения и сокрытия преступления, направленных на оказание

---

[14] Постановление Карачаевского городского суда Карачаево-Черкесской Республики от 05.12.2019 № 1-153/2019 по делу № 1-153/2019.

* Meta признана экстремистской организацией на территории РФ.

психологического воздействия на сознание и поведение людей, создание условий, необходимых для дистанционного хищения чужого имущества. Применение указанных методов позволяет преступнику создать такие условия, при которых жертва: 1) самостоятельно выполняет перевод денежных средств на определенный банковский счет, принадлежащий третьим лицам, либо под контролем преступников совершает иные финансовые операции; 2) добровольно предоставляет преступникам удаленный доступ к управлению электронным устройством либо передает код из SMS-сообщений от банка, подтверждающий финансовую операцию, реквизиты банковской карты, в том числе CVC2/CVV2-код, логины и пароли от сервиса дистанционного банковского обслуживания, а также иную информацию, необходимую для хищения чужого имущества.

Содержание методов социальной инженерии, применяемых при совершении хищений с использованием информационно-телекоммуникационных технологий, включает в себя: психологические приемы манипуляции, связанные с использованием специально подготовленного сценария или текста, предусматривающего исполнение определенной роли при осуществлении преступных действий в целях оказания воздействия на психоэмоциональное состояние жертвы для изменения ее восприятия и убеждения в необходимости срочного принятия решения в ограниченный период времени; технологические приемы манипуляции, направленные на создание поддельного интернет-сайта, фишинговой ссылки и/или использование определенных программных средств для дистанционного воздействия на жертву, обеспечивающих сокрытие преступных действий (deepfake-технологии, программы для изменения голоса, подмены номера телефона, предоставления удаленного доступа к компьютерному или мобильному устройству, вредоносное программное обеспечение и др.).

2.4. Сокрытие следов хищений электронных денежных средств

Согласно криминалистическим учениям, сокрытие отражает содержание так называемого полноструктурного способа совершения преступления, объединяющего способы осуществления всех стадий преступного замысла. По содержательной стороне способы сокрытия преступления можно разделить на следующие группы: утаивание информации и/или ее носителей; уничтожение информации и/или ее носителей; маскировка информации и/или ее носителей; фальсификация информации и/или ее носителей; смешанные способы (Аверьянова и др. 2000, 718–719).

Особенностью способов совершения хищений является то, что в их структуру всегда включаются действия по сокрытию преступных деяний, заключающиеся в маскировке истинных намерений субъектов преступления, демонстрации перед потерпевшим возможностей мошенников, выполнении действий, оставляющих минимум следов, а также уничтожении возникших следов (Драпкин, Карагодин 2011).

Изучение материалов судебной и следственной практики позволило определить содержание основных способов сокрытия хищений, совершенных с применением методов социальной инженерии и информационно-телекоммуникационных технологий.

2.4.1. Сокрытие идентификационных данных

Злоумышленник при совершении хищений использует мобильные устройства, сим-карты, банковские карты, личные кабинеты, электронные кошельки, иные технические средства и предметы, которые оформлены на несуществующих либо третьих лиц, не причастных к совершению преступления (полученные в результате утраты, продажи, передачи сим-карт, банковских карт, личной информации третьим лицам и т. п.) (Макаров, Кузнецов 2020). Как отмечалось выше, преступники осуществляют сокрытие абонентского номера телефона, используя программы, позволяющие осуществлять подмену абонентского номера. Также производятся сокрытие голоса с помощью специальных программных средств, направленных на изменение голоса путем искажения за счет его цифровой обработки (Лебедева 2020), сокрытие IP-адреса в связи с использованием в ходе реализации преступной деятельности VPN-сервисов (анонимайзеров), выполняющих подключение к услугам сети Интернет от IP-адреса, находящегося вне юрисдикции РФ.

Кроме того, при подключении услуг сотовой связи, сети Интернет, банковских продуктов преступник может осуществлять сокрытие реальных идентификационных данных при заключении договора на оказание услуг. Также этот вид преступной деятельности отличается тем, что деяния осуществляются в различных регионах России, т. е. выбор жертв хищений обусловливается их территориальной отдаленностью от преступника, а это существенно противодействует расследованию.

2.4.2. Сокрытие движения похищенных денежных средств по банковским счетам

Преступники после совершения хищения осуществляют многократный быстрый перевод денежных средств на различные подконтрольные счета несколько раз. Указанные финансовые операции осуществляются с целью сокрытия движения денежных средств от правоохранительных органов. Однако и на этих счетах денежные средства не задерживаются и в скором времени обналичиваются.

Обналичивание и вывод похищенных денежных средств происходят через граждан РФ — «дропов», которых умышлено используют организаторы мошеннических кол-центров в преступных целях. Так, в отчете Сбербанка России «Анализ системы вывода денежных средств, похищенных у граждан»[15] выделяются лица, способствующие обналичиванию денежных средств. К их числу отнесены лица, осведомленные о криминальном характере своей деятельности, и лица, которые вовлечены в преступный бизнес неосознанно и используются организаторами преступной схемы под различными легендами (например, через фиктивное трудоустройство). Например, на сайтах поиска работы размещается объявление о наборе сотрудников; кандидату предлагается выпустить банковскую карту для зачисления зарплаты, подключить к ней телефон «работодателя»; далее банковская карта оказывается оформленной на это лицо, а доступ к ней и ее конфиденциальные данные предоставляются участникам преступной группы.

[15] «Анализ системы вывода денежных средств, похищенных у граждан». *Официальный сайт Сбербанка России*. Дата обращения 1 февраля, 2024. http://www.sberbank.ru/ru/person/kibrary/investigations/analiz-sistemy_vyvoda_denezhnyh_sredstv.

Также в указанном отчете выделяются лица, которые самостоятельно обналичивают похищенные денежные средства, зачисленные на их банковские карты или счета в банкоматах и офисах банка; лица-посредники, которые принимают перевод похищенных денежных средств на свои банковские карты и счета, после чего переводят их дальше по цепочке на реквизиты, указанные организатором группы; лица, которые получают наличные денежные средства от других «дропов» и вносят эти средства на свои банковские счета (карты).

2.4.3. Уничтожение следов, укрытие орудий совершения преступлений

Данный способ сокрытия характеризуется следующими действиями: уничтожение сим-карт, банковских карт, электронных устройств; удаление информации, которая содержится в памяти названных устройств, например электронных баз данных, медиафайлов, истории посещения интернет-страниц в браузере, собранных сведений о жертвах преступлений, аккаунтов в электронной почте и социальных сетях, с использованием которых осуществлялось хищение денежных средств, переписок и др. Для сокрытия преступники также блокируют сим-карты, с которых осуществлялись звонки потерпевшим или рассылка SMS-сообщений, веб-сайты, где обманывали потерпевших; обналичивают и закрывают банковские счета, на которые осуществлялся перевод похищенных денежных средств, и др.

3. Выводы

Изучение зарубежных и отечественных источников, содержащих информацию о хищениях, совершенных с применением методов социальной инженерии и информационно-телекоммуникационных технологий, а также эмпирических данных, позволило обобщить особенности способов совершения хищений анализируемой категории.

Способы совершения хищений с применением методов социальной инженерии и информационно-телекоммуникационных технологий в общем виде являются полноструктурными, поскольку в их содержание включен определенный набор действий (этапов).

Первый этап — подготовка — характеризуется следующими действиями: отбор соучастников преступления, оснащение «рабочих мест», приискание необходимых электронных устройств, создание сценариев и алгоритмов обмана, формирование навыков оказания психологического воздействия, сбор информации о потенциальных жертвах. Данный этап включает приискание специальных программ, обеспечивающих последующее сокрытие криминалистически значимой информации о личности преступника и иных обстоятельствах совершения преступления (голоса, внешности, абонентского номера телефона, данных IP-адреса, данных об аккаунте в социальных сетях, финансовых операций, а также действий, выполняемых программами удаленного администрирования на устройстве жертвы).

Второй этап — непосредственное совершение противоправных действий — наряду с применением методов социальной инженерии характеризуется использованием средств сотовой и иных видов голосовой связи, программ удаленного ад-

министрирования, интернет-сайтов, сервисов электронной почты и мгновенного обмена сообщениями, приложений социальных сетей.

Третий этап — сокрытие следов преступления — характеризуется уничтожением сим-карт, электронных устройств, сокрытием движения по банковским счетам похищенных денежных средств, удалением собранных данных о жертвах, переписок, интернет-сайтов, интернет-магазинов, аккаунтов в социальных сетях, программных средств, с использованием которых осуществлялось хищение, и др.

Данный единый комплекс действий преступника, совершающего подобные преступления, выявленный на основе судебно-следственной практики, демонстрирует использование методов социальной инженерии как на этапе подготовки к совершению хищений, так и при непосредственном совершении и сокрытии преступных действий. Между способами совершения рассматриваемых преступлений и другими элементами механизма преступной деятельности, прежде всего обстановкой совершения деяния и характеристикой личности подозреваемого (обвиняемого), потерпевшего, существует непосредственная связь. Кроме того, предложенные способы совершения хищений показывают взаимосвязь между виктимным поведением потерпевших и избранием преступником способа реализации противоправного деяния.

Представленная обобщенная и систематизированная классификация способов совершения хищений рассматриваемой категории может служить основой для разработки мер борьбы с преступностью обозначенного вида и дальнейших междисциплинарных исследований в этой области, а также представляет большое криминалистическое значение при раскрытии и расследовании хищений, совершаемых с использованием методов социальной инженерии и информационно-телекоммуникационных технологий. Данная классификация может быть использована в процессе построения следственных версий, а также учитываться для эффективного планирования комплекса оперативно-разыскных мероприятий и следственных действий.

Библиография

Аверьянова, Татьяна В., Рафаил С. Белкин, Юрий Г. Корухов, Елена Р. Россинская. 2000. *Криминалистика*. М.: Норма.

Драпкин, Леонид Я., Валерий Н. Карагодин. 2011. *Криминалистика.* М.: Проспект

Комиссарова, Ярослава В. 2016. *Криминалистическое изучение личности*. М.: Проспект.

Кравец, Евгений Г., Николай В. Шувалов. 2020. «Комплекс специальных знаний, необходимых при расследовании хищений, совершаемых с использованием вредоносных компьютерных программ». *Юридическая наука и правоохранительная практика* 3 (53): 119–126.

Кравченко, Александр В. 2019. «Психологические механизмы социальной инженерии при совершении преступлений». *Психология и педагогика служебной деятельности* 1: 46–50.

Крылов, Павел. 2019. «Удаленка по собственному желанию». *Group IB.* Дата обращения 1 февраля, 2024. https://blog.group-ib.ru/teamviewerfraud.

Лебедева, Антонина К. 2020. «Проблемы производства судебной фоноскопической экспертизы в свете развития цифровых технологий». *Вестник Университета имени О. Е. Кутафина* 6 (70): 62–71.

Лихтер, Павел Л. 2020. «Технологии астротурфинга с точки зрения права». *Legal Concept* 4: 131–136.

Макаров, Роман А., Александр А. Кузнецов. 2020. «Следственная профилактика хищений с банковских карт, совершаемых дистанционно с использованием средств сотовой связи». *Алтайский юридический вестник* 4 (32): 144–150.
Овчинский, Владимир С. 2016. *Мафия. Новые мировые тенденции Коллекция изборского клуба*. М.: Книжный мир.
Рачева, Нелли В., Федор В. Балеевских, Вячеслав В. Котов. 2021 «Современные способы совершения мошенничества в отношении имущества физических лиц с использованием интернет-ресурсов и технологий социальной инженерии». *Юридическая наука* 2: 101–105.
Ревенков, Павел В., Александр А. Бердюгин. 2017. «Социальная инженерия как источник рисков в условиях дистанционного банковского обслуживания». *Национальные интересы: приоритеты и безопасность* 9 (354): 1747–1760.
Резник, Юрий М. 1994. «Социальная инженерия: предметная область и границы применения». *Социологические исследования* 2: 87–96.
Старостенко, Нина И. 2023. «Первоначальный этап расследования хищений, совершенных с применением методов социальной инженерии и информационно-телекоммуникационных технологий». Дис. … канд. юрид. наук, Краснодарский университет МВД России.
Blommaert, Jan, Tope Omoniyi. 2006. "E-mail fraud: Language, technology, and the indexicals of globalization". *Social Semiotics* 16: 573–605.
Huang, Wilson, Atkins Brockman. 2011. "Social engineering exploitations in online communications: Examining persuasions used in fraudulent e-mails". *Crime online: Correlates, causes, and context.* Ed. by Thomas Holt, 87–111. Durham: Carolina Academic Press.
King, Adam, Thomas, Jim. 2009. "You can't cheat an honest man: Making sense of the Nigerian e-mail scams". *Crimes of the Internet.* Eds Frank Schmallegar, John Pittaro, 206–224. Saddle River: Pearson Education.
Mann, Ian 2008. "Hacking the human: Social engineering techniques and security measures. Burlington". London Routledge: Gower Publishing Company.
Ross, Derek. 2009. "ARS dictaminis perverted: The personal solicitation e-mail as a genre". *Journal of Technical Writing and Communication* 39 (1): 25–41.
Workman, Michael. 2009. "Wisecracker: A theory-grounded investigation of phishing and pretext social engineering threats to information security". *Journal of Personality and Social Psychology* 59 (4): 662–674.
Zook, Matthew 2007. "Your urgent assistance is requested: The intersection of 419 spam and new networks of imagination". *Ethics Place and Environment* 10: 65–88.

Статья поступила в редакцию 22 июля 2021 г.;
рекомендована к печати 2 ноября 2023 г.

Контактная информация:

Старостенко Нина Игоревна — канд. юрид. наук; nstarostenko1996@mail.ru

Forensic features of methods of committing theft using methods of social engineering and information and telecommunication technologies

N. I. Starostenko

Krasnodar University of the Ministry of Internal Affairs of Russia,
128, ul. Yaroslavskaya, Krasnodar, 350005, Russian Federation

For citation: Starostenko, Nina I. 2024. "Forensic features of methods of committing theft using methods of social engineering and information and telecommunication technologies". *Vestnik of Saint Petersburg University. Law* 1: 152–170. https://doi.org/10.21638/spbu14.2024.110 (In Russian)

The article presents a forensic characteristic of the system of actions of a criminal in preparing, committing and concealing thefts committed using methods of social engineering and

information and telecommunication technologies. This article has three main goals. Firstly, it will identify the main types of theft using methods of social engineering and information and telecommunication technologies, which were identified based on the study of judicial and investigative practice. Secondly, it presents the main methods of social engineering that are most often used by criminals to establish psychological contact and influence the psyche and behavior of victims. Thirdly, the analysis of the methods will allow us to identify natural connections between the methods of committing these thefts and other elements of the criminalistic characteristics, in particular the personality of the criminal, the personality of the victim, the mechanism of trace formation, etc. The first part of the main study presents a forensic characteristic of the personality of the criminal and his illegal activities. Next, based on special literature and forensic investigative practice, a forensic classification of methods of committing thefts using social engineering methods and information and telecommunication technologies is formulated. In conclusion, the results of the study are summed up and it is concluded that, in general, the methods under consideration are full-structural, since their content includes a certain set of actions (stages) (preparation, direct commission of illegal actions, concealment of traces of a crime).

Keywords: forensics, crime investigation, social engineering, social engineering methods, remote fraud, methods of committing thefts, information and telecommunication technologies.

References

Aver'ianova, Tat'iana V., Rafail S. Belkin, Iurii G. Korukhov, Elena R. Rossinskaia. 2000. *Forensics*. Moscow, Norma Publ. (In Russian)

Blommaert, Jan, Tope Omoniyi. 2006. "E-mail fraud: Language, technology, and the indexicals of globalization". *Social Semiotics* 16: 573–605.

Drapkin, Leonid Ia., Valerii N. Karagodin. 2011. *Forensics.* Moscow, Prospekt Publ. (In Russian)

Huang, Wilson, Atkins Brockman. 2011. "Social engineering exploitations in online communications: Examining persuasions used in fraudulent e-mails". *Crime online: Correlates, causes, and context.* Ed. by Thomas Holt, 87–111. Durham, Carolina Academic Press.

Komissarova, Iaroslava V. 2016. *Forensic study of personality*. Moscow, Prospekt Publ. (In Russian)

Kravchenko, Aleksandr V. 2019. "Psychological mechanisms of social engineering in the commission of crimes". *Psikhologiia i pedagogika sluzhebnoi deiatel'nosti* 1: 46–50. (In Russian)

Kravets, Evgenii G., Nikolai V. Shuvalov. 2020. "A set of special knowledge required when investigating thefts committed using malicious computer programs". *Iuridicheskaia nauka i pravookhranitel'naia praktika* 3 (53): 119–126. (In Russian)

Krylov, Pavel. 2019. "Remote work at your own request." *Group IB*. Accessed February 1, 2024. https://blog.group-ib.ru/teamviewerfraud. (In Russian)

Lebedeva, Antonina K. 2020. "Problems of forensic phonoscopic examination in the light of the development of digital technologies". *Vestnik Universiteta imeni O. E. Kutafina* 6 (70): 62–71. (In Russian)

Likhter, Pavel L. 2020. "Astroturfing technologies from a legal perspective". *Legal Concept* 4: 131–136. (In Russian)

Makarov, Roman A., Aleksandr A. Kuznetsov. 2020. "Investigative prevention of thefts from bank cards committed remotely using cellular communications". *Altaiskii iuridicheskii vestnik* 4 (32): 144–150. (In Russian)

Mann, Ian 2008. "Hacking the human: Social engineering techniques and security measures. Burlington". London Routledge, Gower Publishing Company.

Ovchinskii, Vladimir S. 2016. *Mafia. New world trends Collection of the Izborsk club.* Moscow, Knizhnyi mir Publ. (In Russian)

Racheva, Nelli V., Fedor V. Baleevskikh, Viacheslav V. Kotov. 2021 "Modern ways to increase fraud against the property of individuals using Internet resources and social engineering technologies". *Iuridicheskaia nauka* 2: 101–105. (In Russian)

Revenkov, Pavel V., Aleksandr A. Berdiugin. 2017. "Social engineering as a source of risks in the conditions of remote banking services". *Natsional'nye interesy: prioritety i bezopasnost'* 9 (354): 1747–1760. (In Russian)
Reznik, Iurii M. 1994. "Social engineering: Subject area and boundaries of application". *Sotsiologicheskie issledovaniia* 2: 87–96. (In Russian)
Ross, Derek. 2009. "ARS dictaminis perverted: The personal solicitation e-mail as a genre". *Journal of Technical Writing and Communication* 39 (1): 25–41.
Starostenko, Nina I. 2023. "The initial stage of the investigation of thefts committed using methods of social engineering and information and telecommunication technologies". PhD Thesis in Law, Krasnodarskii universitet MVD Rossii. (In Russian)
King, Adam, Thomas, Jim. 2009. "You can't cheat an honest man: Making sense of the Nigerian e-mail scams". *Crimes of the internet Saddle River.* Eds Frank Schmallegar, John Pittaro, 206–224. New Jersey, Pearson Education.
Workman, Michael. 2009. "Wisecracker: A theory-grounded investigation of phishing and pretext social engineering threats to information security". *Journal of Personality and Social Psychology* 59 (4): 662–674.
Zook, Matthew 2007. "Your urgent assistance is requested: The intersection of 419 spam and new networks of imagination". *Ethics Place and Environment* 10: 65–88.

Received: July 22, 2021
Accepted: November 2, 2023

Author's information:

Nina I. Starostenko — PhD in Law; nstarostenko1996@mail.ru